(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108734813 B
(45)授权公告日 2022.08.23

(21)申请号 201710255812.4
(22)申请日 2017.04.19
(65)同一申请的已公布的文献号
申请公布号 CN 108734813 A
(43)申请公布日 2018.11.02
(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层
(72)发明人 卓松 李俊聪 朱佳 范铭 彭诗辉 贾镕企 罗挺
(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 熊永强 贾允
(51)Int.Cl.
G07C 9/22(2020.01)

审查员 马彦

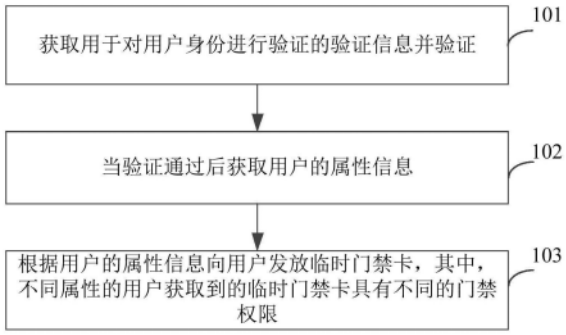
权利要求书4页 说明书18页 附图13页

(54)发明名称

临时门禁卡的发放方法及装置

(57)摘要

本发明提出一种临时门禁卡的发放方法及装置,其中,方法包括:获取用于对用户身份进行验证的验证信息并验证;当验证通过后获取用户的属性信息;根据用户的属性信息向用户发放临时门禁卡;其中,不同属性的用户获取到的临时门禁卡具有不同的门禁权限。由此,通过对用户身份进行验证的验证信息进行验证通过后,针对不同用户发放具有不同门禁权限的临时卡,操作简单便捷,准确性高,从而提高了临时门禁卡发放的安全性。



CN 108734813 B

1.一种临时门禁卡的发放方法,其特征在于,包括:

在用户忘带长期门禁卡的情况下,获取用于对用户身份进行验证的验证信息并验证;

当验证通过后获取所述用户的属性信息,其中,所述属性信息获得方式具体为:

人脸图像作为验证信息,获取用户的属性信息包括从人脸数据库中获取第一用户的属性信息,将第一用户的属性信息作为用户的属性信息;

或,应用程序扫描二维码验证并结合移动终端的标识生成验证信息,获取用户的属性信息包括接收服务器在验证通过后发送的用户的属性信息,其中用户的属性信息是由服务器根据移动终端的标识获取到的;

或,语音信息作为验证信息,获取用户的属性信息包括从语音数据库中获取第二用户的属性信息,将第二用户的属性信息作为用户的属性信息;

或,身份证信息作为验证信息,获取用户的属性信息包括获取与身份证信息对应的第三用户的属性信息,将第三用户的属性信息作为用户的属性信息;

根据所述用户的属性信息向所述用户发放临时门禁卡;其中,预先为不同的属性设置不同的属性标识,以及为不同的门禁权限设置不同的权限标识,利用属性标识和权限标识构建属性与权限之间的对应关系,不同属性的用户获取到的临时门禁卡具有不同的门禁权限,根据所述用户的属性信息查询属性与门禁权限之间的对应关系或根据预先存储的与属性信息相关的处理算法,获取与所述用户的属性信息对应的目标门禁权限;

根据所述目标门禁权限为所述用户生成所述临时门禁卡;

在所述用户获取到所述临时门禁卡后,将所述用户的所述长期门禁卡在所述临时门禁卡的有效期限内设置成失效状态。

2.根据权利要求1所述的临时门禁卡的发放方法,其特征在于,所述获取用于对用户身份进行验证的验证信息并验证,包括:

通过摄像装置采集所述用户的人脸图像作为所述验证信息;

将所述用户的人脸图像与人脸数据库中的人脸图像进行匹配;

如果所述用户的人脸图像与所述人脸数据库中第一用户的人脸图像的第一匹配度超过预设的第一数值时,则通过对所述用户身份的验证;

所述当验证通过后获取所述用户的属性信息,包括:

从所述人脸数据库中获取所述第一用户的属性信息;

将所述第一用户的属性信息作为所述用户的属性信息。

3.根据权利要求2所述的临时门禁卡的发放方法,其特征在于,还包括:

按照预设的第一数据库构建策略,预先构建所述人脸数据库,其中,所述人脸数据库中至少存储有第一用户的人脸图像、所述第一用户的属性信息以及所述第一用户的人脸图像与所述第一用户的属性信息之间的对应关系;

定期对所述人脸数据库进行更新。

4.根据权利要求1所述的临时门禁卡的发放方法,其特征在于,所述获取用于对用户身份进行验证的验证信息并验证,包括:

通过所安装的应用程序的服务器生成二维码;

将所述二维码通过屏幕显示给所述用户,以使所述用户通过移动终端上的所述应用程序扫描所述二维码并结合所述移动终端的标识生成所述验证信息发给所述服务器进行验

证；

所述当验证通过后获取所述用户的属性信息，包括：

接收所述服务器在验证通过后发送的所述用户的属性信息；其中所述用户的属性信息是由所述服务器根据所述移动终端的标识获取到的。

5.根据权利要求1所述的临时门禁卡的发放方法，其特征在于，所述获取用于对用户身份进行验证的验证信息并验证，包括：

通过拾音装置采集所述用户的语音信息作为所述验证信息；

将所述用户的语音信息与语音数据库中的语音信息进行匹配；

如果所述用户的语音信息与所述语音数据库中第二用户的语音信息的第二匹配度超过预设的第二数值时，通过对所述用户身份的验证；

所述当验证通过后获取所述用户的属性信息，包括：

从所述语音数据库中获取所述第二用户的属性信息；

将所述第二用户的属性信息作为所述用户的属性信息。

6.根据权利要求5所述的临时门禁卡的发放方法，其特征在于，还包括：

按照预设的第二数据库构建策略，预先构建所述语音数据库，其中，所述语音数据库中至少存储有第二用户的语音信息、所述第二用户的属性信息以及所述第二用户的语音信息与所述第二用户的属性信息之间的对应关系；

定期对所述语音数据库进行更新。

7.根据权利要求6所述的临时门禁卡的发放方法，其特征在于，还包括：

对所述临时门禁卡的有效期限进行监控。

8.一种临时门禁卡的发放方法，其特征在于，包括：

在用户忘带长期门禁卡的情况下，服务器将用于对用户身份进行验证的二维码发送给第一终端；

所述第一终端通过屏幕将所述二维码显示给用户以使所述用户通过第二终端扫描所述二维码；

所述第二终端将扫描后的所述二维码发送给所述服务器进行验证；

所述服务器在验证通过后获取所述用户的属性信息发给所述第一终端；以及预先为不同的属性设置不同的属性标识，为不同的门禁权限设置不同的权限标识，利用属性标识和权限标识构建属性与权限之间的对应关系，不同属性的用户获取到的临时门禁卡具有不同的门禁权限，根据所述用户的属性信息查询属性与门禁权限之间的对应关系或根据预先存储的与属性信息相关的处理算法，获取与所述用户的属性信息对应的目标门禁权限；以及根据所述目标门禁权限为所述用户生成所述临时门禁卡；以及在所述用户获取到临时门禁卡后，将所述用户的长期门禁卡在所述临时门禁卡的有效期限内设置成失效状态；

所述第一终端根据所述用户的属性信息向所述用户发放所述临时门禁卡。

9.根据权利要求8所述的临时门禁卡的发放方法，其特征在于，所述第二终端将扫描后的所述二维码发送给所述服务器进行验证，包括：

所述第二终端将扫描后的所述二维码和所述第二终端的标识发送给所述服务器；所述服务器根据所述二维码进行身份验证；

所述服务器在验证通过后获取所述用户的属性信息发给所述第一终端，包括：

所述服务器在验证通过后根据所述第二终端的标识获取所述用户的属性信息；

所述服务器将所述用户的属性信息发送给所述第一终端。

10.根据权利要求9所述的临时门禁卡的发放方法，其特征在于，还包括：

所述服务器接收用户发送的基本信息形成用户数据库，其中，所述基本信息中包括所述用户的属性信息和所述第二终端的标识；

所述服务器在 验证通过后根据所述第二终端的标识获取所述用户的属性信息，包括：

所述服务器在验证通过后根据所述第二终端的标识查询所述用户数据库，得到所述用户的属性信息。

11.一种第一终端，其特征在于，包括：

验证模块，用于在用户忘带长期门禁卡的情况下，获取用于对用户身份进行验证的验证信息并验证；

获取模块，用于当验证通过后获取所述用户的属性信息，其中，所述属性信息获得方式具体为：

人脸图像作为验证信息，获取用户的属性信息包括从人脸数据库中获取第一用户的属性信息，将第一用户的属性信息作为用户的属性信息；

或，应用程序扫描二维码验证并结合移动终端的标识生成验证信息，获取用户的属性信息包括接收服务器在验证通过后发送的用户的属性信息，其中用户的属性信息是由服务器根据移动终端的标识获取到的；

或，语音信息作为验证信息，获取用户的属性信息包括从语音数据库中获取第二用户的属性信息，将第二用户的属性信息作为用户的属性信息；

或，身份证信息作为验证信息，获取用户的属性信息包括获取与身份证信息对应的第三用户的属性信息，将第三用户的属性信息作为用户的属性信息；

发放模块，用于根据所述用户的属性信息向所述用户发放临时门禁卡；

其中，预先为不同的属性设置不同的属性标识，以及为不同的门禁权限设置不同的权限标识，利用属性标识和权限标识构建属性与权限之间的对应关系，不同属性的用户获取到的临时门禁卡具有不同的门禁权限，根据所述用户的属性信息查询属性与门禁权限之间的对应关系或根据预先存储的与属性信息相关的处理算法，获取与所述用户的属性信息对应的目标门禁权限；

根据所述目标门禁权限为所述用户生成所述临时门禁卡；

在所述用户获取到所述临时门禁卡后，将所述用户的所述长期门禁卡在所述临时门禁卡的有效期限内设置成失效状态。

12.一种门禁卡发放系统，其特征在于，包括：

服务器，用于在用户忘带长期门禁卡的情况下，将用于对用户身份进行验证的二维码发送给第一终端，接收用户所使用的第二终端发送的所述二维码并进行验证，在验证通过后获取所述用户的属性信息下发给所述第一终端；

所述第一终端，用于接收所述二维码并通过屏幕将所述二维码显示给用户以使所述用户通过第二终端扫描所述二维码，以及接收所述服务器在对所述用户的验证通过后下发的所述用户的属性信息，并根据所述用户的属性信息向所述用户发放临时门禁卡；

所述第二终端，用于扫描所述二维码并发送给所述服务器进行验证；

其中，预先为不同的属性设置不同的属性标识，以及为不同的门禁权限设置不同的权限标识，利用属性标识和权限标识构建属性与权限之间的对应关系，不同属性的用户获取到的临时门禁卡具有不同的门禁权限，根据所述用户的属性信息查询属性与门禁权限之间的对应关系或根据预先存储的与属性信息相关的处理算法，获取与所述用户的属性信息对应的目标门禁权限；

根据所述目标门禁权限为所述用户生成所述临时门禁卡；

在所述用户获取到所述临时门禁卡后，将所述用户的所述长期门禁卡在所述临时门禁卡的有效期限内设置成失效状态。

13.一种计算机可读存储介质，包括计算机指令，其特征在于，所述计算机指令被处理器执行时实现如权利要求1-7任一或权利要求8-10任一所述的临时门禁卡的发放方法。

临时门禁卡的发放方法及装置

技术领域

[0001] 本发明涉及信息处理技术领域，尤其涉及一种临时门禁卡的发放方法及装置。

背景技术

[0002] 在企业场景中，员工忘带门禁卡的情况每天都在发生，员工在申请领取临时门禁卡时，主要通过在前台手动登记基本信息，然后由前台人员对员工的身份进行验证后发放一个临时门禁卡。

[0003] 现有由前台人工为员工发放临时门禁卡，可能存在难以正确识别员工身份或者识别错误的情况时有发生，导致临时门禁卡发放存在很大的安全隐患。

发明内容

[0004] 本发明提出一种临时门禁卡的发放方法及其装置，用于解决现有由前台人工为员工发放临时门禁卡，可能存在难以正确识别员工身份或者识别错误的情况时有发生，导致临时门禁卡发放存在很大的安全隐患的问题。

[0005] 本发明第一方面实施例提出了一种临时门禁卡的发放方法，包括以下步骤：获取用于对用户身份进行验证的验证信息并验证；当验证通过后获取所述用户的属性信息；根据所述用户的属性信息向所述用户发放临时门禁卡；其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0006] 本发明第二方面实施例提出了一种临时门禁卡的发放方法，包括：服务器将用于对用户身份进行验证的二维码发送给第一终端；所述第一终端通过屏幕将所述二维码显示给用户以使所述用户通过第二终端扫描所述二维码；所述第二终端将扫描后的所述二维码发送给所述服务器进行验证；所述服务器在验证通过后获取所述用户的属性信息发给所述第一终端；所述第一终端根据所述用户的属性信息向所述用户发放临时门禁卡；其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0007] 本发明第三方面实施例提出了一种第一终端，包括：验证模块，用于获取用于对用户身份进行验证的验证信息并验证；获取模块，用于当验证通过后获取所述用户的属性信息；发放模块，用于根据所述用户的属性信息向所述用户发放临时门禁卡；其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0008] 本发明第四方面实施例提出了一种门禁卡发放系统，包括：服务器，用于将用于对用户身份进行验证的二维码发送给第一终端，接收用户所使用的第二终端发送的所述二维码并进行验证，在验证通过后获取所述用户的属性信息下发给所述第一终端；所述第一终端，用于接收所述二维码并通过屏幕将所述二维码显示给用户以使所述用户通过第二终端扫描所述二维码，以及接收所述服务器在对所述用户的验证通过后下发的所述用户的属性信息，并根据所述用户的属性信息向所述用户发放临时门禁卡；所述第二终端，用于扫描所述二维码并发送给所述服务器进行验证；其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0009] 本发明实施例提供的技术方案可以包括以下有益效果：

[0010] 通过对用户身份进行验证的验证信息进行验证通过后，针对不同用户发放具有不同门禁权限的临时卡，操作简单便捷，准确性高，从而提高了临时门禁卡发放的安全性。

[0011] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0012] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0013] 图1为本发明实施例提供的一种临时门禁卡的发放方法的流程示意图；

[0014] 图2为本发明实施例提供的第二种临时门禁卡的发放方法的流程示意图；

[0015] 图3为本发明实施例提供的获取人脸图像的示意图；

[0016] 图4为本发明实施例提供的一个图像上传的过程示意图；

[0017] 图5为本发明实施例提供的第三种临时门禁卡的发放方法的流程示意图；

[0018] 图6为本发明实施例提供的二维码显示方式的示意图；

[0019] 图7为本发明实施例提供的第四种临时门禁卡的发放方法的流程示意图；

[0020] 图8为本发明实施例提供的第五种临时门禁卡的发放方法的流程示意图；

[0021] 图9为本发明实施例提供的一种目前门禁权限的获取方法的流程示意图；

[0022] 图10为本发明实施例提供的第六种临时门禁卡的发放方法的流程示意图；

[0023] 图11为本发明实施例提供的选择不同的流程进行身份验证的示意图；

[0024] 图12为本发明实施例提供的第七种临时门禁卡的发放方法的流程示意图；

[0025] 图13为本发明实施例提供的一种临时门禁卡的识别方法的流程示意图；

[0026] 图14为本发明实施例提供的另一种临时门禁卡的识别方法的流程示意图；

[0027] 图15为本发明实施例的一个临时门禁卡处理的流程交互图；

[0028] 图16(a)为本发明实施例的信息确认示意图；

[0029] 图16(b)为本发明实施例的输入分机号的示意图；

[0030] 图16(c)为本发明实施例的通知信息示意图；

[0031] 图17为本发明实施例提供的一种第一终端的结构示意图；

[0032] 图18为本发明实施例提供的一种门禁卡发放系统的结构示意图；

[0033] 图19为本发明实施例提供的一种门禁识别装置的结构示意图；

[0034] 图20为本发明实施例提供的另一种门禁识别装置的结构示意图；

[0035] 图21为本发明实施例提供的一种第一终端的结构示意图；

[0036] 图22为本发明实施例提供的一种门禁卡发放系统的结构示意图；

[0037] 图23为本发明实施例提供的一种门禁识别装置的结构示意图。

具体实施方式

[0038] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本发明，而不能理解为对本发明的限制。

[0039] 下面参考附图描述本发明实施例的临时门禁卡的发放方法及装置。

[0040] 具体地，不论是生活场景中，业主忘带门禁卡，需要通过在门卫处手动登记基本信息，然后由门卫对业主身份进行验证后发放一个临时门禁卡，业主通过该临时门禁卡能够进入居住单元楼以及乘电梯去相对应的楼层；还是企业场景中，员工忘带门禁卡，需要通过前台人员对员工的身份进行验证后发放一个临时门禁卡，员工通过该临时门禁卡能够进入办公楼以及相对应的办公室。

[0041] 因此，为了方便忘带门禁卡的用户，需要向其发放临时门禁卡。本发明提供了一种临时门禁卡的发放方法，需要注意的是，与现有技术的发放临时门禁卡方法相比，本实施例不需要人工对用户身份进行验证，准确性更高，而且针对不同用户发放具有不同门禁权限的临时卡，安全性高。

[0042] 为了便于描述，下面首先集中在终端侧(比如自助机侧)描述本发明实施例的临时门禁卡的发放方法。

[0043] 需要说明的是，本实施例中的终端可以铺设在企业办公楼、居民楼等。

[0044] 具体地，图1为本发明实施例提供的第一种临时门禁卡的发放方法的流程示意图。如图1所示，该临时门禁卡的发放方法包括以下步骤：

[0045] S101，获取用于对用户身份进行验证的验证信息并验证。

[0046] 具体地，在对用户身份进行验证时，需要获取对用户身份进行验证的验证信息，并对验证信息进行验证。需要说明的是，可以根据具体应用场景不同采用不同的方式获取用于对用户身份进行验证的验证信息并验证，举例说明如下：

[0047] 第一种示例，通过摄像装置采集用户的人脸图像作为验证信息，将用户的人脸图像与人脸数据库中的人脸图像进行匹配，如果用户的人脸图像与人脸数据库中第一用户的人脸图像的第一匹配度超过预设的第一数值时，则通过对用户身份的验证。

[0048] 第二种示例，通过所安装的应用程序的服务器生成二维码，将二维码通过屏幕显示给用户，以使用户通过移动终端上的应用程序扫描二维码并结合移动终端的标识生成验证信息发给服务器进行验证。

[0049] 第三种示例，通过拾音装置采集用户的语音信息作为验证信息，将用户的语音信息与语音数据库中的语音信息进行匹配，如果用户的语音信息与语音数据库中第二用户的语音信息的第二匹配度超过预设的第二数值时，通过对用户身份的验证。

[0050] 第四种示例，通过扫描装置扫描获取用户的身份证信息作为验证信息，查询数据库中是否存在身份证信息，如果存在身份证信息，则通过对用户身份的验证。

[0051] 第五种示例，通过终端屏幕上带有的虚拟键盘，输入与用户相关的身份信息，例如身份证、手机号等信息作为验证信息，然后查询数据库，如果存在上述验证信息，则通过对用户身份的验证。例如，当用户为一个访客时，可以通过虚拟键盘输出一个预约码作为验证信息。当用户为一个员工时，可以同虚拟键盘输入自身的身份证信息或者手机号码作为验证信息。

[0052] 需要注意的是，以上对获取用于对用户身份进行验证的验证信息并验证方式仅为举例说明，可以根据实际应用需要进行选择和调整。

[0053] S102，当验证通过后获取用户的属性信息。

[0054] 具体地，在验证通过后，为了准确向用户发放临时门禁卡，则需要获取用户的属性

信息。其中，可以根据实际应用场景需要，选择不同的验证方式，采用不同的验证方式，获取用户的属性信息不同，举例说明如下：

[0055] 第一种示例，人脸图像作为验证信息，获取用户的属性信息包括从人脸数据库中获取第一用户的属性信息，将第一用户的属性信息作为用户的属性信息。

[0056] 第二种示例，应用程序扫描二维码验证并结合移动终端的标识生成验证信息，获取用户的属性信息包括接收服务器在验证通过后发送的用户的属性信息，其中用户的属性信息是由服务器根据移动终端的标识获取到的。

[0057] 第三种示例，语音信息作为验证信息，获取用户的属性信息包括从语音数据库中获取第二用户的属性信息，将第二用户的属性信息作为用户的属性信息。

[0058] 第四种示例，身份证信息作为验证信息，获取用户的属性信息包括获取与身份证信息对应的第三用户的属性信息，将第三用户的属性信息作为用户的属性信息。

[0059] 需要说明的是，以上方式仅为当验证通过后获取用户的属性信息的举例说明，可以根据实际应用需要选择或者设置其他的方式。

[0060] S103，根据用户的属性信息向用户发放临时门禁卡，其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0061] 具体地，在获取用户的属性信息后，需要根据用户的属性信息向用户发放临时门禁卡。即根据属性信息确定用户相对应的门禁权限后，向用户发送相对应权限的临时门禁卡。由此，进一步提高临时门禁卡发送的安全性。

[0062] 需要说明的是，可以根据实际应用场景需要，采用不同的方式根据用户的属性信息向用户发放临时门禁卡，举例说明如下：

[0063] 第一种示例，预先设置用户的属性信息查询属性与门禁权限之间的对应关系，进而根据用户的属性信息，查询该对应关系获取对应的目标门禁权限。进一步地，根据目标门禁权限为用户生成临时门禁卡，将门禁卡以实体卡片或者虚拟卡片(可以在移动终端等便携设备中显示)形式向用户发放临时门禁卡。

[0064] 第二种示例，预先存储与属性信息相关的处理算法，在确定用户的属性信息后，获取与预存的处理算法相关的参数进行计算，确定与该属性信息对应的目标门禁权限，以及根据目标门禁权限为用户生成临时门禁卡，将门禁卡以实体卡片或者虚拟卡片(可以在移动终端等便携设备中显示)形式向用户发放临时门禁卡。

[0065] 需要说明的是，以上方式仅为根据用户的属性信息向用户发放临时门禁卡的举例说明，可以根据实际应用需要选择或者设置其他的方式。

[0066] 综上所述，本发明实施例的临时门禁卡的发放方法，通过对用户身份进行验证的验证信息进行验证通过后，针对不同用户发放具有不同门禁权限的临时卡，操作简单便捷，准确性高，从而提高了临时门禁卡发放的安全性。

[0067] 基于以上实施例，为了更加清楚的描述如何获取用于对用户身份进行验证的验证信息并验证，当验证通过后获取用户的属性信息，通过图2-图6所示实施例具体说明如下：

[0068] 图2为本发明实施例提供的第二种临时门禁卡的发放方法的流程示意图。

[0069] 本实施例是根据人脸图像作为验证信息，将人脸图像与人脸数据库中的人脸图像进行匹配验证通过后，从人脸数据库中获取第一用户的属性信息作为用户的属性信息。

[0070] 具体说明如图2所示，即上述实施例中的步骤S101包括：S201-S203；步骤S102包

括:S204-S205。

[0071] S201,通过摄像装置采集用户的人脸图像作为验证信息。

[0072] S202,将用户的人脸图像与人脸数据库中的人脸图像进行匹配。

[0073] S203,当用户的人脸图像与人脸数据库中第一用户的人脸图像的第一匹配度超过预设的第一数值时,则通过对用户身份的验证。

[0074] 具体地,自助机上设置有摄像装置,用户可以通过手动、语音等方式触发摄像装置开始工作,并采集用户的人脸图像作为验证信息。其中,摄像装置获取人脸图像的方式有很多种,可以根据实际应用需要进行选择设置。

[0075] 作为一种实现形式,如图3所示,摄像装置在检测到当前用户的面部到达预设区域时,触发定位灯亮起,提示当前用户的双眼在预设时间内直视定位灯,并在当前用户的双眼直视定位灯的过程中采集对应的人脸图像。其中,预设区域是预先设置的能够进行面部识别的区域,即当前用户的面部进入该预设区域内表示面部识别模块可以开始采集工作。

[0076] 进而,将获取的人脸图像与人脸数据库中的人脸图像进行匹配。其中,人脸数据库是预先构建好并存储的。在本实施例中,按照预设的第一数据库构建策略,预先构建人脸数据库。

[0077] 需要说明的是,人脸数据库中至少存储有第一用户的人脸图像、第一用户的属性信息以及第一用户的人脸图像与第一用户的属性信息之间的对应关系。

[0078] 需要说明的是,根据不同的应用场景,其第一数据构建策略不同以保证信息安全和识别效率。以企业场景作为一种示例,可以采用组织结构分组的形式进行构建策略,首先访问人力资源部接口获取员工的姓名、组织结构和头像等属性信息并保存,接着将员工组织结构去重(比如员工A既属于组织结构B又属于组织结构C,将A员工属于组织结构C删除),根据组织结构创建人脸数据库,最后对员工信息进行遍历,根据组织结构,将员工的姓名和头像创建到组织架构对应的人脸数据库中。

[0079] 在实际应用中,比如上述的企业场景中,存在员工变动情况,需要定期对人脸数据库进行更新,以确保临时门禁卡发放的安全性。继续以企业场景作为一种示例,从相关数据库中获取前一天记录的所有员工,再通过访问人力资源部接口获取当前员工记录,比较员工的组织结构是否有变更,在有变更的情况下,需要对员工信息进行更新,同时比较员工状态,将离职人员从人脸数据库总删除,将刚入职人员更新到人脸数据库中。

[0080] 其中,定期可以是一天、两天等,根据实际应用需要选择设置。

[0081] 具体地,在人脸识别时,将用户的人脸图像与人脸数据库中的人脸图像进行匹配,即将用户的人脸图像特征数据与人脸数据库中的人脸图像特征数据进行匹配,若比较获知匹配结果超过预设的第一数值,则确定当前用户的身份具有合法性,例如该第一数值可以为95%。

[0082] 进一步地,人脸数据库中至少存储有第一用户的属性信息,还可以包括第一用户的其他信息,例如,手机号码、身份证信息、分机号、年龄、性别等基本信息。其中,用户的手机号码、身份证信息、分机号等可以作为用户的标识信息。

[0083] 当用户的人脸图像与人脸数据库中第一用户的人脸图像的第一匹配度不超过预设的第一数值时,则通过对用户身份的验证具体包括以下步骤:

[0084] 获取用户的标识信息。比如上述的企业场景中,可以进一步地要求用户输入其他

的标识信息，可以为用户的座机分机号，或者手机号码，以确定出该用户对应的第一用户。

[0085] 在获取到用户的标识信息后，可以将获取到的标识信息，与人脸数据库中第一用户的标识信息进行比较，当两者的标识信息一致时，则可以通过对用户身份的验证。

[0086] 举例说明，可以提示用户输入手机号码，为了进一步提高身份验证的准确性，在上述两者的标识信息一致时，进一步根据用户的输入的手机号码，发送一条微信到用户的手机上，用户通过微信中的链接进行二次确认，确认通过后判定为用户本人后，再通过对用户身份的验证。本实施例中，在人脸识别的基础上引入手机号码的二次验证，改变传统的单一识别模式，为识别提供更丰富的应用场景，安全性更高。

[0087] 需要说明的是，当用户在人脸识别失败的情况下，进一步选择其它方式进行验证通过后，可以主动向用户推送信息(不限于短信、微信形式)，提醒用户上传最新头像，用户通过推送信息中的链接可以直接进行头像上传操作，提升下一次人脸验证识别率。

[0088] 图4为本发明实施例提供的一个图像上传的过程示意图，如图4所示：

[0089] 具体地，用户通过点开推送信息链接后，在用户面前显示如图4中左边界面所示，提醒用户为了提升自助机人脸识别准确性，即避免下一次识别失败的情况出现，用户可以点击“上传照片”上传符合免冠、无墨迹、清晰和光线均匀等要求的图片。在用户点击“上传照片”后，可以选择合适照片上传，上传的结果如图4中间界面所示，用户通过点击“确认上传”完成照片上传，显示上传成功界面，如图4右边界面所示。可以理解的是，在图4中间界面所示，用户还可以通过点击“重新拍照”，实时获取用户的照片进行上传，进一步提升人脸识别的准确性。

[0090] 本实施例中，在人脸识别的过程中可以形成一个闭环，在识别后可以主动通知，并且可以提醒用户上传最近的用户人脸图像，让整个识别流程形成闭环，提高识别效率。

[0091] 需要说明的是，当上述两者的标识信息不一致时，判定为非用户本人。

[0092] 实际应用中当人脸数据库中存在两个面貌相似的两个第一用户时，当将用户的人脸图像与人脸数据库中的人脸图像进行匹配时，就可以能出现用户的人脸图像与两个第一用户的人脸图像的第一匹配度超出预设的第一数值的情况，此时，为了提高临时门禁卡发放的准确性，需要进一步地验证用户的其他信息，例如可以为用户的手机号码后四位、分机号码等，从而两个第一用户中确定出与用户对应的第一用户。例如，用户X有两个第一用户A和B，则用户X输入的分机号码为4567，而在人脸数据库中第一用户A的分机号码为0123，而第一用户B的分机号码为4567，则可以确定出用户X与第一用户B对应，即将第一用户B的属性信息作为用户X的属性信息。

[0093] S204，从人脸数据库中获取第一用户的属性信息。

[0094] S205，将第一用户的属性信息作为用户的属性信息。

[0095] 具体地，在验证通过后，即确定人脸图像与人脸数据库中的用户X的人脸图像匹配，从人脸数据库中获取用户X的属性信息。在获取到第一用户的属性信息并将其作为用户的属性信息。

[0096] 本实施例中，以企业场景为例，属性信息可以为用户的岗位类型，也可以为用户的员工类型等。本实施例中，可以为不同的岗位设置不同的级别，不同的级别可以对应不同的门禁权限。不同的岗位可以包括人事岗位、行政岗位等。或者，可以为不同的员工类型设置不同的级别，员工类型可以包括：销售人员、管理人员等。再例如，用户还可以分为在职员

工、实行员工或者访客等，访客的相关信息以及图像也可以预先存储到人脸数据库中。

[0097] 作为一种示例，根据岗位级别设置对应的门禁权限，比如普通工作人员具有开启所在办公室门的权限；部门经理具有开启所在部门所有办公室门的权限。另外还针对不同部门设置对应的门禁权限，比如行政部门的员工具有开启会议室门的权限；研发部门具有开启实验室门的权限。以及针对访客可以设置具有进入公司闸门以及电梯的权限等。

[0098] 图5为本发明实施例提供的第三种临时门禁卡的发放方法的流程示意图。

[0099] 本实施例是根据应用程序扫描二维码并结合移动终端的标识生成验证信息发给服务器验证，并在验证通过后服务器根据移动终端的标识获取到用户的属性信息。

[0100] 具体说明如图5所示，即上述实施例中的步骤S101包括：S301-S302；步骤S102包括：S303。

[0101] S301，通过所安装的应用程序的服务器生成二维码。

[0102] S302，将二维码通过屏幕显示给用户，以使用户通过移动终端上的应用程序扫描二维码并结合移动终端的标识生成验证信息发给服务器进行验证。

[0103] 具体地，自助机将所属位置、自身名称以及一个随机数等信息提供给安装的应用程序的服务器，服务器对上述信息进行编码，生成带链接地址的二维码通过屏幕显示给用户，如图6所示。

[0104] 进而，用户可以通过第二终端(如图6中所示的手机，也可以是平板电脑、智能手表等)的应用程序(如图6所示的微信，也可以是QQ等)扫描二维码，并结合移动终端的标识(不同的用户对应的移动终端的标识不同，由此能够确定用户的唯一性)生成验证信息发给服务器进行验证。

[0105] 具体地，服务器根据验证信息能够验证移动终端的权限，即用户是否有访问权限。

[0106] S303，接收服务器在验证通过后发送的用户的属性信息；其中用户的属性信息是由服务器根据移动终端的标识获取到的。

[0107] 具体地，在服务器验证通过后，能够接收到服务器发送的用户的属性信息，即服务根据移动终端的标识查找与其对应的用户，并获取其属性信息。

[0108] 本实施例中，服务器可以预先对用户的基本信息进行采集，例如用户的属性信息、手机号码、移动终端的标识码、身份证信息、分机号、年龄、性别等基本信息进行采集。以企业场景为例，企业可以在服务器中注册一个公众号，员工可以对该公众号进行关注，然后填写自己的基本信息，这样就完成了对员工的信息采集。进一步地，访客类的用户也可以对该公众号进行关注，然后在公众号下选择预约并填写相关的基本信息。

[0109] 图7为本发明实施例提供的第四种临时门禁卡的发放方法的流程示意图。

[0110] 本实施例是将语音信息作为验证信息，将语音信息与语音数据库中的语音信息进行匹配验证通过后，从语音数据库中获取第二用户的属性信息作为用户的属性信息。

[0111] 具体说明如图7所示，即上述实施例中的步骤S101包括：S401-S203；步骤S402包括：S404-S405。

[0112] S401，通过拾音装置采集用户的语音信息作为验证信息。

[0113] S402，将用户的语音信息与语音数据库中的语音信息进行匹配。

[0114] S403，当用户的语音信息与语音数据库中第二用户的语音信息的第二匹配度超过预设的第二数值时，通过对用户身份的验证。

[0115] 具体地，自助机上设置有拾音装置，用户可以通过手动等方式触发拾音装置开始工作，并采集用户的语音信息(比如用户根据界面提供文本朗读一段话、或者是随便说一段话)作为验证信息。

[0116] 进而，将获取的语音信息与语音信息库中的语音信息进行匹配。更具体地，通过语音信息进行处理，接着提取声纹特征，建立相关声纹模型，最后声纹比对以确定是否匹配。并在用户的语音信息与语音数据库中第二用户的语音信息的第二匹配度超过预设的第二数值时通过对用户身份的验证。

[0117] 其中，语音数据库是预先构建好并存储的。在本实施例中，按照预设的第二数据库构建策略，预先构建语音数据库。

[0118] 需要说明的是，语音数据库中至少存储有第二用户的语音信息、第二用户的属性信息以及第二用户的语音信息与第二用户的属性信息之间的对应关系。

[0119] 需要说明的是，根据不同的应用场景，其第二数据构建策略不同以保证信息安全和识别效率。第二数据构建策略可以与第一数据构建策略相同，可以根据组织结构来构建语音数据库，关于语音数据库的构建过程可参见人脸数据库的构建过程，此处不再赘述。

[0120] 进一步地，语音数据库中至少存储有第二用户的属性信息，还可以包括第二用户的其他信息，例如，手机号码、身份证信息、分机号、年龄、性别等基本信息。其中，用户的手机号码、身份证信息、分机号等可以作为用户的标识信息。

[0121] 当用户的语音信息与语音数据库中第二用户的语音信息的第二匹配度超过预设的第二数值时，则通过对用户身份的验证具体包括以下步骤：

[0122] 获取用户的标识信息。比如上述的企业场景中，可以进一步地要求用户输入其他的标识信息，可以为用户的座机分机号，或者手机号码的后四位，以确定出该用户对应的第二用户。

[0123] 在获取到用户的标识信息后，可以将获取到的标识信息，与语音数据库中第二用户的标识信息进行比较，当两者的标识信息一致时，则可以通过对用户身份的验证。

[0124] 实际应用中存在两个语音相似的两个第二用户，当将用户的语音信息与语音数据库中的语音信息进行匹配时，就可以能出现用户的人脸图像与两个第二用户的人脸图像的第二匹配度超出预设的第二数值的情况，此时，为了提高临时门禁卡发放的准确性，需要进一步地验证用户的其他信息，例如可以为用户的手机号码后四位、分机号码等，从而两个第二用户中确定出与用户对应的第二用户。例如，用户X有两个第二用户C和D，则用户X输入的分机号码为4567，而在人脸数据库中第二用户C的分机号码为0123，而第二用户D的分机号码为4567，则可以确定出用户X与第二用户D对应，即将第二用户D的属性信息作为用户X的属性信息。

[0125] 可以理解的是，如果用户的语音信息与语音数据库中第二用户的语音信息的第二匹配度不超过预设的第二数值时，不通过对用户身份的验证。

[0126] S404，从语音数据库中获取第二用户的属性信息。

[0127] S405，将第二用户的属性信息作为用户的属性信息。

[0128] 具体地，在验证通过后，即确定人脸图像与语音数据库中的用户Y的语音信息匹配，从语音数据库中获取用户Y的属性信息，并将其作为用户的属性信息。关于属性信息的介绍可参见上述实施例中实施例中相关内容的记载，此处不再赘述。

[0129] 综上所述，本发明实施例的临时门禁卡的发放方法，通过不同的方式对用户身份进行验证的验证信息进行验证通过后，针对不同用户发放具有不同门禁权限的临时卡，操作简单便捷，准确性高，从而提高了临时门禁卡发放的效率、安全性高，降低人工成本。

[0130] 图8为本发明实施例提供的第五种临时门禁卡的发放方法的流程示意图，在步骤S102后，该临时门禁卡的发放方法还包括：

[0131] S501，根据用户的属性信息查询属性与门禁权限之间的对应关系，获取与用户的属性信息对应的目标门禁权限。

[0132] 具体地，预先为不同的属性设置不同的属性标识，以及为不同的门禁权限设置不同的权限标识，利用属性标识和权限标识构建属性与权限之间的对应关系。进一步地，该对应关系中还包括权限的存储地址，即在存储地址对应的存储空间中存储有权限的具体内容。也就是说，对应关系中包括属性标识、权限标识以及存储地址之间的映射关系。

[0133] 图9为根据用户的属性信息查询属性与门禁权限之间的对应关系，获取与用户的属性信息对应的目标门禁权限的流程示意图，具体包括以下步骤：

[0134] S5011，根据用户的属性标识查询到对应关系，获取与属性标识对应的目标门禁权限的权限标识。

[0135] 具体地，可以按照上述实施例记载的方法获取用户的属性信息，该用户的属性信息为属性标识。

[0136] S5012，从所述对应关系中查询与权限标识对应的存储地址。

[0137] S5013，根据存储地址定位存储空间，从存储空间中读取目标门禁权限。

[0138] 本实施例中，预先为不同的门禁权限设置不同的存储空间，每个存储空间具有一个存储地址，在该存储空间中存储有门禁权限的具体内容。在根据目标门禁权限的权限标识，从对应关系中可以获取到该目标门禁权限的权限标识的存储地址后，从而可以定位到该存储地址对应的存储空间，然后从该存储空间中读取到目标门禁权限的具体内容。

[0139] S502，根据目标门禁权限为用户生成临时门禁卡。

[0140] 具体地，预先存储属性与门禁权限之间的对应关系，根据获取的用户信息属性查询该对应关系，获取与用户的属性信息对应的目标门禁权限，并根据目标门禁权限为用户生成临时门禁卡。即临时门禁卡能够针对不同用户具有不同的权限。

[0141] 需要说明的是，在生成门禁临时卡后，将门禁卡以实体卡片或者虚拟卡片(可以在移动终端等便携设备中显示)形式向用户发放临时门禁卡。

[0142] 在将临时门禁卡发放给用户后，可以对临时门禁卡的有效期限进行监控，并且在用户获取到临时门禁卡后，将该用户所拥有的长期门禁卡在临时门禁卡的有效期限内设置成失效状态，从而保证在同一时刻一个用户只能使用一张门禁卡进入公司，可以提高安全性。

[0143] S503，将临时门禁卡的标识以及所具有的目标门禁权限发送给门禁系统，以使门禁系统对临时门禁卡的标识与所具有的目标门禁权限进行关联注册。

[0144] 本实施例中，可以将门禁卡的标识以及所具有的目标门禁权限发送给门禁系统，门禁系统收到临时门禁卡的标识后，将临时门禁卡的标识与所具有的目标门禁权限进行关联注册。

[0145] 实际应用中，当用户使用门禁临时卡时，门禁系统能够对其进行相应处理，具体

地，读取门禁卡标识，判断其是否具有允许进入的权限，如果有允许进入，如果没有，可以通过语音、鸣笛等方式进行提示。其中，临时门禁卡的标识是指能够确定唯一门禁卡，具有唯一性。

[0146] 需要说明的是，为了进一步提高安全性，临时门禁卡具有有效期限，比如具体为8小时、24小时等。

[0147] S504，将临时门禁卡的有效期限发给门禁系统，以使门禁系统对临时门禁卡的有效性进行监控。

[0148] 具体地，不同的临时门禁卡可能具有不同的有效期限。由此，需要将临时门禁卡的有效期发给门禁系统，门禁系统能够对有效期内的具有权限的临时门禁卡允许进入；对不在有效期内的所有临时门禁卡都禁止进入。比如，临时门禁卡的有效期为24小时，超过24小时后，该门禁卡不再具有权限，有效提升临时门禁卡发放的安全性。门禁系统可以根据该有效期限对临时门禁卡的门禁权限进行回收，当临时门禁卡的有效期限到期后，门禁系统可以将临时门禁卡的门禁权限消除，或者该临时门禁卡处于失效状态。

[0149] 图10为本发明实施例提供的第六种临时门禁卡的发放方法的流程示意图。如图10所示，该临时门禁卡的发放方法包括以下步骤：

[0150] S601，服务器将用于对用户身份进行验证的二维码发送给第一终端，第一终端通过屏幕将二维码显示给用户，以使用户通过第二终端扫描二维码，第二终端将扫描后的二维码发送给服务器进行验证。

[0151] 具体地，用户可以通过根据自己身份选择不同的流程进行身份验证，如图11所示，在一个企业场景中，如果用户是访客身份可以选择点击左边的“已约访客”开始验证流程；如果用户是员工身份，可以选择点击右边的“员工启动”开始验证流程。

[0152] 进而，当用户根据实际需要开始选择后(比如根据自己员工身份点击图11中的“员工启动”)，将用于对用户身份进行验证的二维码发送给第一终端，第一终端通过屏幕显示给用户(如上述实施例中的图6所示)。可以理解的是，生成二维码才能够显示，由此，在将二维码通过屏幕显示给用户之前，需要接收应用程序的服务器生成并发送的二维码。

[0153] 进而，用户可以通过第二终端(不限于手机、平板电脑和智能佩戴设备等中的一种或者多种)上的应用程序(不限于微信、QQ和微博等中的一种或者多种)扫描二维码并发给应用程序的服务器进行验证。

[0154] 具体地，第二终端将扫描后的二维码和第二终端的标识发送给服务器；服务器根据二维码进行身份验证，服务器在验证通过后获取用户的属性信息发给第一终端，包括：服务器在验证通过后根据第二终端的标识获取用户的属性信息，服务器将用户的属性信息发送给第一终端。

[0155] 可以理解的是，服务器预先存储有用户的属性信息，作为一种实现方式，服务器接收用户发送的基本信息形成用户数据库，其中，基本信息中包括用户的属性信息和第二终端的标识。由此，在服务器验证通过后根据第二终端的标识获取用户的属性信息，包括：服务器在验证通过后根据第二终端的标识查询用户数据库，得到用户的属性信息。

[0156] S602，服务器在验证通过后获取用户的属性信息发给第一终端。

[0157] 具体地，服务器在验证通过后，返回给第一终端用户的属性信息。

[0158] S603，第一终端根据用户的属性信息向用户发放临时门禁卡，其中，不同属性的用

户获取到的临时门禁卡具有不同的门禁权限。

[0159] 具体地，在获取用户的属性信息后，需要根据用户的属性信息向用户发放临时门禁卡。即根据属性信息确定用户相对应的门禁权限后，向用户发送相对应权限的临时门禁卡。由此，进一步提高临时门禁卡发送的安全性。

[0160] 需要说明的是，可以根据实际应用场景需要，第一终端采用不同的方式根据用户的属性信息向用户发放临时门禁卡，举例说明如下：

[0161] 第一种示例，第一终端根据预先设置用户的属性信息查询属性与门禁权限之间的对应关系，进而根据用户的属性信息，查询该对应关系获取对应的目标门禁权限，以根据目标门禁权限为用户生成临时门禁卡，将门禁卡以实体卡片或者虚拟卡片(可以在移动终端等便携设备中显示)形式向用户发放临时门禁卡。

[0162] 第二种示例，第一终端根据预先存储与属性信息相关的处理算法，在确定用户的属性信息后，获取与预存的处理算法相关的参数进行计算，确定与该属性信息对应的目标门禁权限，以及根据目标门禁权限为用户生成临时门禁卡，将门禁卡以实体卡片或者虚拟卡片(可以在移动终端等便携设备中显示)形式向用户发放临时门禁卡。

[0163] 需要说明的是，以上方式仅为根据用户的属性信息向用户发放临时门禁卡的举例说明，可以根据实际应用需要选择或者设置其他的方式。

[0164] 以第一种示例为例，向用户发放临时门禁卡、以及将门禁卡的标识以及所具有的目标门禁权限发送给门禁系统(门禁系统收到临时门禁卡的标识后，将临时门禁卡的标识与所具有的目标门禁权限进行关联注册)。由此，当用户使用门禁临时卡时，门禁系统能够对其进行相应(即读取门禁卡标识，判断其是否具有允许进入的权限，如果有允许进入，如果没有，可以通过语音、鸣笛等方式进行提示)。其中，临时门禁卡的标识是指能够确定唯一门禁卡，具有唯一性。

[0165] 需要说明的是，为了进一步提高安全性，临时门禁卡具有有效期限，比如具体为8小时、24小时等。

[0166] 具体地，不同的临时门禁卡可能具有不同的有效期限。由此，需要将临时门禁卡的有效期发给门禁系统，门禁系统能够对有效期内的具有权限的临时门禁卡允许进入；对不在有效期内的所有临时门禁卡都禁止进入。比如，临时门禁卡的有效期为24小时，超过24小时后，该门禁卡不再具有权限，有效提升临时门禁卡发放的安全性。

[0167] 综上所述，本发明实施例的临时门禁卡的发放方法，通过服务器将用于对用户身份进行验证的二维码发送给第一终端，接着第一终端通过屏幕显示给用户，以使用户通过第二终端扫描二维码并发给应用程序的服务器进行验证，并在验证通过后获取用户的属性信息发给第一终端，最后第一终端根据用户的属性信息向用户发放临时门禁卡，其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限，操作简单便捷，准确性高，从而提高了临时门禁卡发放的安全性。

[0168] 为了更加全面的说明本发明实施例的临时门禁卡的发放方法，下面集中以应用程序(比如微信、QQ等)服务器侧描述本发明实施例的临时门禁卡的发放方法。

[0169] 图12为本发明实施例提供的第七种临时门禁卡的发放方法的流程示意图。如图12所示，该临时门禁卡的发放方法包括以下步骤：

[0170] S701，接收用户的移动终端发送用于对用户身份进行验证的验证信息，验证信息

中包括二维码和移动终端的标识。

[0171] S702,根据验证信息中的二维码进行身份验证。

[0172] 具体地,应用程序服务器预先需要对具体终端(比如自助机)所属地址、终端标识以及随机数等信息进行编码生成二维码并发送给终端显示。

[0173] 进而,能够接收用户通过扫描二维码的方式发送的验证信息(包括二维码和移动终端的标识)。由此,根据验证信息中的二维码进行身份验证。即扫描二维码后,通过应用程序的相关接口(比如微信的openid)验证移动终端的权限完成身份验证。

[0174] S703,在验证通过后根据移动终端的标识获取用户的属性信息。

[0175] S704,将用户的属性信息发送给终端,以使终端根据属性信息向用户发放临时门禁卡,其中,不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0176] 需要说明的是,应用程序服务器预先接收用户发送的基本信息(包括用户的属性信息和移动终端的标识)并形成用户数据库。

[0177] 进而,在验证通过后,根据移动终端的标识查询用户数据库,获取用户的属性信息发送给终端,以使针对不同属性的用户发放卡具有不同的门禁权限的临时门禁卡。

[0178] 综上所述,本发明实施例的临时门禁卡的发放方法,通过接收用户的移动终端发送用于对用户身份进行验证的包括二维码和移动终端的标识的验证信息,并根据验证信息中的二维码进行身份验证,然后在验证通过后根据移动终端的标识获取用户的属性信息发送给终端,以使针对不同属性的用户发放卡具有不同的门禁权限的临时门禁卡。由此,操作简单便捷、准确性高,从而提高了临时门禁卡发放的安全性且降低人工成本。

[0179] 基于上述实施例,为了更加清楚描述在向用户发送临时门禁卡之后,门禁装置如何针对不同权限的临时门禁卡进行不同的操作控制,下面以门禁装置侧集中描述一种临时门禁卡的识别方法。

[0180] 图13为本发明实施例提供的一种临时门禁卡的识别方法的流程示意图。如图13所示,该临时门禁卡的识别方法包括以下步骤:

[0181] S801,获取临时门禁卡的门禁权限。

[0182] 具体地,在对临时门禁卡具有开启目标门的权限进行判断时,需要获取临时门禁卡的门禁权限。需要说明的是,可以根据具体应用场景不同采用不同的方式获取临时门禁卡的门禁权限,举例说明如下:

[0183] 第一种示例,接收目标门发送的临时门禁卡的标识,根据临时门禁卡的标识查询临时门禁卡的标识与所具有的门禁权限之间的关联关系,获取到临时门禁卡的门禁权限。作为一种场景举例说明目标门如何获取临时门禁卡标识:用户通过刷卡的方式(门禁临时卡是实体卡片),使得目标门获取临时门禁卡的标识。作为另一种场景举例说明目标门如何获取临时门禁卡标识:用户通过移动终端与目标门建立连接发送临时门禁卡标识,使得目标门获取临时门禁卡的标识(可以针对临时门禁卡是虚拟卡片的情况)。

[0184] 第二种示例,用户通过移动终端直接将临时门禁卡的标识发送给门禁装置,进而,门禁装置根据临时门禁卡的标识查询临时门禁卡的标识与所具有的门禁权限之间的关联关系,获取到临时门禁卡的门禁权限。

[0185] 需要注意的是,以上对获取临时门禁卡的门禁权限方式仅为举例说明,可以根据实际应用需要进行选择和调整。

[0186] 可以理解的是，预先保存有各临时门禁卡的标识以及所具有的门禁权限的关联关系才能够根据临时门禁卡的标识获取其具有的门禁权限。具体地，在本实施例中，可以接收终端发送的各临时门禁卡的标识以及所具有的门禁权限，并根据各临时门禁卡的标识与所具有的门禁权限，建立关联关系。

[0187] S802，根据门禁权限判断是否临时门禁卡具有开启目标门的权限。

[0188] S803，当判断出临时门禁卡具有开启目标门的权限时，则开启目标门。

[0189] 具体地，根据获取的门禁权限可以判断临时门禁卡是否具有开启目标门的权限，在临时门禁卡具有开启目标门的权限时，开启目标门。可以理解的是，在临时门禁卡不具有开启目标门的权限时，保持目标门关闭状态。

[0190] 需要说明的是，临时门禁卡具有有效期限。需要接收临时门禁卡的有效期限，并根据有效期限对临时门禁卡的有效性进行监控。

[0191] 作为一种示例，在判断出临时门禁卡具有开启目标门的权限时，需要进一步根据有效期限判断临时门禁卡是否具有有效性，在临时门禁卡具有有效性时开启目标门；在在临时门禁卡不具有有效性时，保持目标门关闭状态。

[0192] 综上所述，本发明实施例的临时门禁卡的识别方法，通过获取临时门禁卡的门禁权限，并根据门禁权限判断是否临时门禁卡具有开启目标门的权限，最后当判断出临时门禁卡具有开启目标门的权限时开启目标门。由此，通过提高识别效率，方便用户使用，并根据临时门禁卡有效期进行有效监控，进一步提高安全性。

[0193] 图14为本发明实施例提供的另一种临时门禁卡的识别方法的流程示意图，在步骤S803后，该临时门禁卡的识别方法还包括：

[0194] S901，在用户获取到临时门禁卡后，将用户的长期门禁卡在临时门禁卡的有效期限内设置成失效状态。

[0195] S902，回收临时门禁卡，删除临时门禁卡中的门禁权限。

[0196] 具体地，在发放临时门禁卡后，需要将该用户其它门禁卡(比如长期门禁卡)在临时门禁卡有效期限内设置成失效状态。以确保一用户只能通过一卡进入相对应的目标地点，提高安全性。

[0197] 具体地，可以根据具体应用场景针对不同的情况回收临时门禁卡，举例说明如下：

[0198] 第一种示例，在用户归还临时门禁卡时将该临时门禁卡中的门禁权限删除。

[0199] 第二种示例，临时门禁卡超出有效期限时将该临时门禁卡中的门禁权限删除。

[0200] 需要注意的是，以上针对不同的情况回收临时门禁卡仅为举例说明，可以根据实际应用需要进行选择和调整。

[0201] 由此，通过在用户获取到临时门禁卡后，将用户的长期门禁卡在临时门禁卡的有效期限内设置成失效状态和回收临时门禁卡，删除临时门禁卡中的门禁权限，进一步提高安全性。

[0202] 图15为本发明实施例的一个临时门禁卡处理的流程交互图。

[0203] 参见图15，以企业场景为例说明，本实施例包括：员工、自助机、微信、访客系统、人脸系统、门禁系统以及通闸。本实施例通过设备之间的信息交互举例描述本实施例提供的临时门禁卡发放、识别的流程的具体应用场景，具体说明如下：

[0204] 需要说明的是，自助机能够进行生成微信验证二维码、抓取人脸图像、发放临时工

卡、还卡等操作。微信公众号主要针对员工身份鉴权。访客系统主要验证员工身份。人脸系统主要是通过人脸检测来验证员工身份。门禁系统主要进行注册门禁权限、验证门禁权限、回收门禁权限等操作。

[0205] 具体地，员工进入公司发现忘记携带门禁卡，可以通过触发自助机生成二维码和自助机上的摄像装置拍照两种方式进行身份验证以发放临时门禁卡。下面分两种示例，分别描述上述两种方式的具体验证过程。

[0206] 示例一，在生成二维码后，员工可以通过移动终端上安装的微信执行扫描二维码操作，通过微信验证员工身份，并在验证通过后发放临时门禁卡。

[0207] 为了本领域人员更加清楚如何通过微信验证员工身份的具体过程，下面结合图16(a)具体说明如下：

[0208] 具体地，通过微信对二维码(如上述实施例中的图6所示)进行扫描后，如图16(a)所示，员工进入手机身份确认页面，访问系统通过微信的openid验证手机权限，即非员工手机号不允许进行访问，员工在手机上确认身份，访客系统将本次确认保存到缓存同时设置失效时间(比如1分钟、两分钟)。

[0209] 需要说明的是，自助机预先将所属地址、标识(比如名称、序列号等)和随机数等信息发送到访客系统，访客系统将上述信息编码，生成带链接地址的二维码。由此，员工扫描二维码后能进入相关验证界面。

[0210] 具体地，为了进一步保证安全性，自助机每预设时间(比如3秒)，再次将所属地址、标识(比如名称、序列号等)和随机数等信息发送到访客系统进行循环，访客系统从缓存中查询结果，确认员工身份后，将确认结果通知给自助机，自助机收到确认结果后进行临时门禁卡打印(即上述实施例中的临时门禁卡发放)。

[0211] 示例二，在启动摄像装置进行拍照后，人脸系统通过人脸图像检测员工身份后，在自助机上显示输入分机号界面，并在分机号输入正确后发放临时门禁卡。

[0212] 为了本领域人员更加清楚如何通过人脸图像验证员工身份的具体过程，具体说明如下：

[0213] 具体地，员工可以选择自己对应的组织结构，自助机通过调用系统(比如avicap32.dll)开始摄像装置，员工将面部对准摄像头(如上述实施例中的图3所示)，自助机通过系统的截屏功能，截取拍摄区域人脸图像。

[0214] 进而，自助机将人脸图像发送到访客系统，访客系统调用人脸系统对人脸图像进行检测，确认为人脸后，通过员工组织结构在预设的人脸数据库中找到对应的人脸图像，并进行匹配，将匹配度超过预设阈值即成功的结果返回给自助机。

[0215] 进而，通过人脸图像检测员工身份后，在自助机上显示输入分机号界面，比如图16(b)所示，“请输入五位数的分机号”，并在分机号输入正确后发放临时门禁卡。

[0216] 具体地，在发放临时门禁卡结束后，可以通过微信信息的方式(可以是预先设置好自动回复方式)通知员工已经领取过临时门禁卡以进一步确保安全性。显示界面可以如图16(c)所示。

[0217] 可以理解的是，在发放临时门禁卡之前，还需要确定员工的门禁权限，即可以通过员工的工卡号等方式作为员工的标识发送给访客系统，访客系统通过门禁装置提供的接口验证工卡号的权限，并将结果返回自助机。即针对不同员工发放不同门禁权限的临时门禁

卡。

[0218] 需要说明的是，新卡是没有具体权限的，需要通过刷卡器向门禁装置进行登记授权等方式给新卡赋予不同的权限成为临时门禁卡保存在自助机中。

[0219] 进而，自助机接收到员工的工卡号对应的权限时，通过调用打印机接口打印对应的临时门禁卡。可以理解的是，本实施例中的临时门禁卡是实体卡片形式的。

[0220] 需要说明的是，在打印的过程中，如果发现临时门禁卡未授权，将其进行回收，停止打印。

[0221] 需要说明的是，访客系统预设周期(比如每天)对已经发放的临时门禁卡进行查询，对员工未进行归还(超过有效期限)的临时门禁卡主动回收权限。

[0222] 由此，能够大大提高员工领取临时门禁卡的效率，缓解了上班高峰期前台工作人员的工作压力，降低人工成本，且能够自动准确发放临时门禁卡，实现门禁权限的自动下放和回收，大大提高了安全性。

[0223] 为了实现上述实施例，本发明还提出一种第一终端。

[0224] 图17为本发明实施例提供的第一种第一终端的结构示意图。该第一终端包括：验证模块11、获取模块12和发送模块13。

[0225] 其中，验证模块11，用于获取用于对用户身份进行验证的验证信息并验证。

[0226] 获取模块12，用于当验证通过后获取用户的属性信息。

[0227] 发放模块13，用于根据用户的属性信息向用户发放临时门禁卡；其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0228] 需要说明的是，前述对临时门禁卡发放方法实施例的解释说明也适用于本实施例的终端，此处不再赘述。

[0229] 综上所述，本发明实施例的第一终端，通过对用户身份进行验证的验证信息进行验证通过后，针对不同用户发放具有不同门禁权限的临时卡，操作简单便捷，准确性高，从而提高了临时门禁卡发放的安全性。

[0230] 图18为本发明实施例提供的一种门禁卡发放系统的结构示意图。该门禁卡发放系统包括：第一终端1、服务器2和第二终端3。

[0231] 其中，服务器2，用于将用于对用户身份进行验证的二维码发送给第一终端1，接收用户所使用的第二终端3发送的二维码并进行验证，在验证通过后获取用户的属性信息下发给第一终端1。

[0232] 第一终端1，用于接收二维码并通过屏幕将二维码显示给用户以使用户通过第二终端3扫描二维码，以及接收服务器2在对用户的验证通过后下发的用户的属性信息，并根据用户的属性信息向用户发放临时门禁卡。

[0233] 第二终端3，用于扫描二维码并发送给服务器2进行验证。

[0234] 其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0235] 需要说明的是，第一终端可以同时具备人脸识别和语言识别的功能，即设置有人脸数据库构建模块和语言数据库构建模块以及各自的更新模块，用户可以根据自己的需求选择使用人脸图像验证还是通过语言信息进行验证，或者通过二维码的方式进行验证。

[0236] 需要说明的是，前述对临时门禁卡发放方法实施例的解释说明也适用于本实施例的门禁卡发放系统，此处不再赘述。

[0237] 综上所述，本发明实施例的门禁卡发放系统，通过服务器将用于对用户身份进行验证的二维码发送给第一终端，接着第一终端通过屏幕显示给用户，以使用户通过第二终端扫描二维码并发给应用程序的服务器进行验证，并在验证通过后获取用户的属性信息发给第一终端，最后第一终端根据用户的属性信息向用户发放临时门禁卡，其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限，操作简单便捷，准确性高，从而提高了临时门禁卡发放的安全性。

[0238] 图19为本发明实施例提供的一种门禁识别装置的结构示意图。该门禁识别装置用于用户使用临时门禁卡试图开启目标门，包括：获取模块41、判断模块42、开启模块43。

[0239] 其中，获取模块41，用于获取临时门禁卡的门禁权限。

[0240] 判断模块42，用于根据门禁权限判断是否临时门禁卡具有开启目标门的权限。

[0241] 开启模块43，用于当判断出临时门禁卡具有开启目标门的权限时，则开启目标门。

[0242] 进一步地，获取模块41，具体用于接收目标门发送的临时门禁卡的标识，根据临时门禁卡的标识查询临时门禁卡的标识与所具有的门禁权限之间的关联关系，获取到临时门禁卡的门禁权限。

[0243] 进一步地，作为一种可能的实现方式，图20为本发明实施例提供的另一种门禁识别装置的结构示意图，如图20所示，在图19的基础上，该门禁识别装置还包括：关联建立模块44、监控模块45和失效设置模块46。

[0244] 其中，关联建立模块41，用于在获取临时门禁卡的门禁权限之前，接收终端发送的各临时门禁卡的标识以及所具有的门禁权限，以及根据各临时门禁卡的标识与所具有的门禁权限，建立关联关系。

[0245] 在本发明的一个实施例中，临时门禁卡具有有效期限，监控模块45，用于接收临时门禁卡的有效期限，根据有效期限对临时门禁卡的有效性进行监控。

[0246] 进一步地，开启模块43，具体用于当判断出临时门禁卡具有开启目标门的权限时，根据有效期限判断临时门禁卡是否具有有效性，如果临时门禁卡具有有效性，则开启目标门。

[0247] 进一步地，失效设置模块46，用于在用户获取到临时门禁卡后，将用户的长期门禁卡在临时门禁卡的有效期限内设置成失效状态。

[0248] 需要说明的是，前述对临时门禁卡识别方法实施例的解释说明也适用于本实施例的门禁识别装置，此处不再赘述。

[0249] 综上所述，本发明实施例的门禁识别装置，通过获取临时门禁卡的门禁权限，并根据门禁权限判断是否临时门禁卡具有开启目标门的权限，最后当判断出临时门禁卡具有开启目标门的权限时开启目标门。由此，通过提高识别效率，方便用户使用，并根据临时门禁卡有效期进行有效监控，进一步提高安全性。

[0250] 为了实现上述实施例，本发明还提出一种终端，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，处理器执行程序时实现上述实施中第一种到第五种临时门禁卡的发放方法。

[0251] 为了实现上述实施例，本发明还提出一种第一终端。

[0252] 图21为本发明实施例提供的一种第一终端的结构示意图。

[0253] 其中，需要说明的是，图21以第一终端侧为例。如图20所示，该第一终端可以包括：

处理器11;用于存储处理器可执行指令的存储器12。其中,处理器11被配置为:获取用于对用户身份进行验证的验证信息并验证;当验证通过后获取用户的属性信息;根据用户的属性信息向用户发放临时门禁卡;其中,不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0254] 图22为本发明实施例提供的一种门禁卡发放系统的结构示意图。

[0255] 其中,需要说明的是,如图22所示,该门禁卡发放系统可以包括:处理器11;用于存储处理器可执行指令的存储器12。其中,处理器11被配置为:服务器将用于对用户身份进行验证的二维码发送给第一终端;第一终端通过屏幕将二维码显示给用户以使用户通过第二终端扫描二维码;第二终端将扫描后的二维码发送给服务器进行验证;服务器在验证通过后获取用户的属性信息发给第一终端;第一终端根据用户的属性信息向用户发放临时门禁卡;其中,不同属性的用户获取到的临时门禁卡具有不同的门禁权限。

[0256] 图23为本发明实施例提供的一种门禁识别装置的结构示意图。

[0257] 其中,需要说明的是,如图23所示,该门禁识别装置可以包括:处理器11;用于存储处理器可执行指令的存储器12。其中,处理器11被配置为:获取临时门禁卡的门禁权限;根据门禁权限判断是否临时门禁卡具有开启目标门的权限;当判断出临时门禁卡具有开启目标门的权限时,则开启目标门。

[0258] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0259] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中,“多个”的含义是至少两个,例如两个,三个等,除非另有明确具体的限定。

[0260] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为,表示包括一个或更多个用于实现定制逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分,并且本发明的优选实施方式的范围包括另外的实现,其中可以不按所示出或讨论的顺序,包括根据所涉及的功能按基本同时的方式或按相反的顺序,来执行功能,这应被本发明的实施例所属技术领域的技术人员所理解。

[0261] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤,例如,可以被认为是用于实现逻辑功能的可执行指令的定序列表,可以具体实现在任何计算机可读介质中,以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用,或结合这些指令执行系统、装置或设备而使用。就本说明书而言,"计算机可读介质"可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下:具有一个或多个布线的电

连接部(电子装置),便携式计算机盘盒(磁装置),随机存取存储器(RAM),只读存储器(ROM),可擦除可编辑只读存储器(EPROM或闪速存储器),光纤装置,以及便携式光盘只读存储器(CDROM)。另外,计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质,因为可以例如通过对纸或其他介质进行光学扫描,接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序,然后将其存储在计算机存储器中。

[0262] 应当理解,本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中,多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。如,如果用硬件来实现和在另一实施方式中一样,可用本领域公知的下列技术中的任一项或他们的组合来实现:具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路,具有合适的组合逻辑门电路的专用集成电路,可编程门阵列(PGA),现场可编程门阵列(FPGA)等。

[0263] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成,所述的程序可以存储于一种计算机可读存储介质中,该程序在执行时,包括方法实施例的步骤之一或其组合。

[0264] 此外,在本发明各个实施例中的各功能单元可以集成在一个处理模块中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。

[0265] 上述提到的存储介质可以是只读存储器,磁盘或光盘等。尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

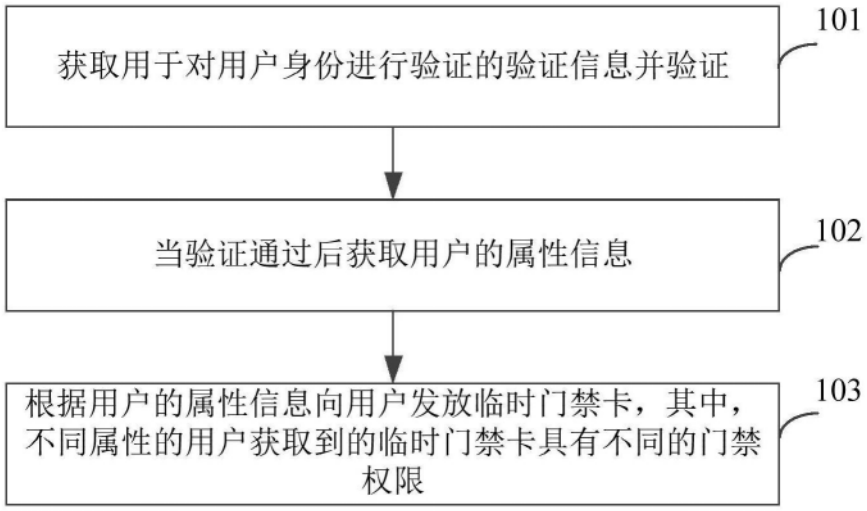

获取用于对用户身份进行验证的验证信息并验证
101
当验证通过后获取用户的属性信息
102
根据用户的属性信息向用户发放临时门禁卡，其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限
103

图1

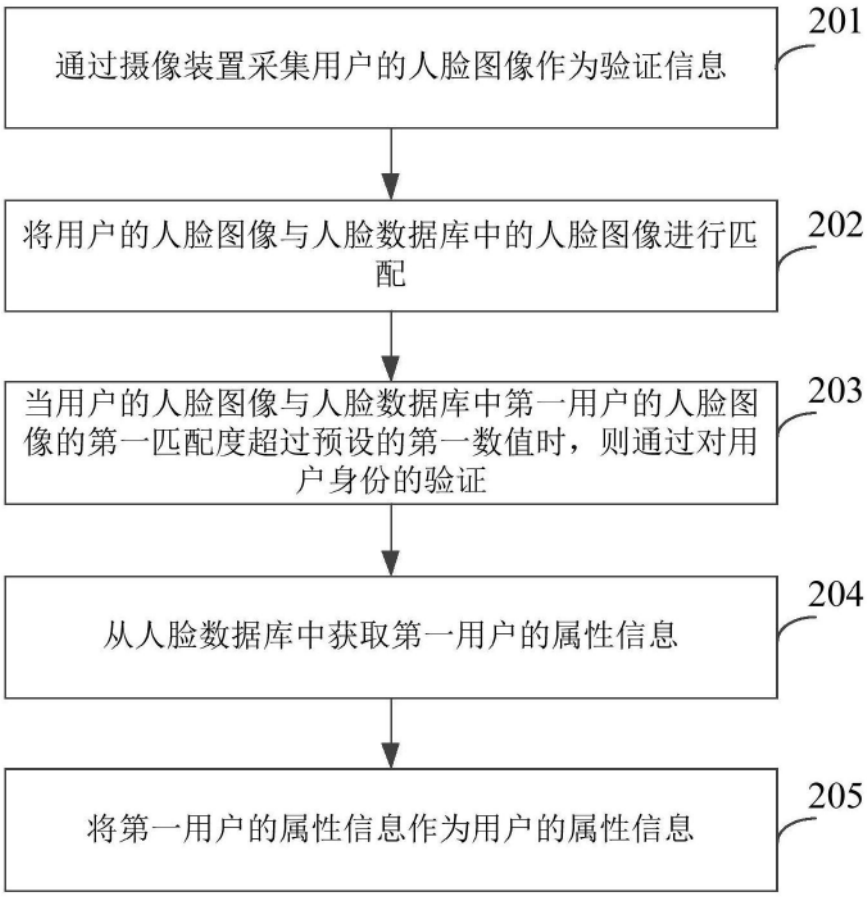

通过摄像装置采集用户的人脸图像作为验证信息
201
将用户的人脸图像与人脸数据库中的人脸图像进行匹配
202
当用户的人脸图像与人脸数据库中第一用户的人脸图像的第一匹配度超过预设的第一数值时，则通过对用户身份的验证
203
从人脸数据库中获取第一用户的属性信息
204
将第一用户的属性信息作为用户的属性信息
205

图2


人脸识别中…

图3


上传近期照片
提升自助机人脸识别准确性
照片要求
（免冠、无墨镜、清晰、光线均匀）
上传照片
确认上传
重新拍照
上传成功
恭喜！
（您可以去自助机尝试使用人脸识别啦）

图4

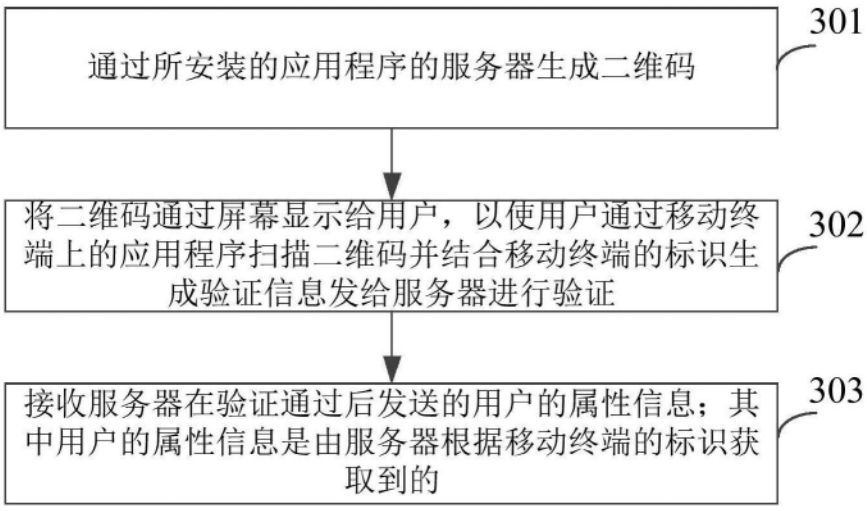

通过所安装的应用程序的服务器生成二维码
301
将二维码通过屏幕显示给用户，以使用户通过移动终端上的应用程序扫描二维码并结合移动终端的标识生成验证信息发给服务器进行验证
302
接收服务器在验证通过后发送的用户的属性信息；其中用户的属性信息是由服务器根据移动终端的标识获取到的
303

图5


请打开微信扫描二维码以识别身份

图6

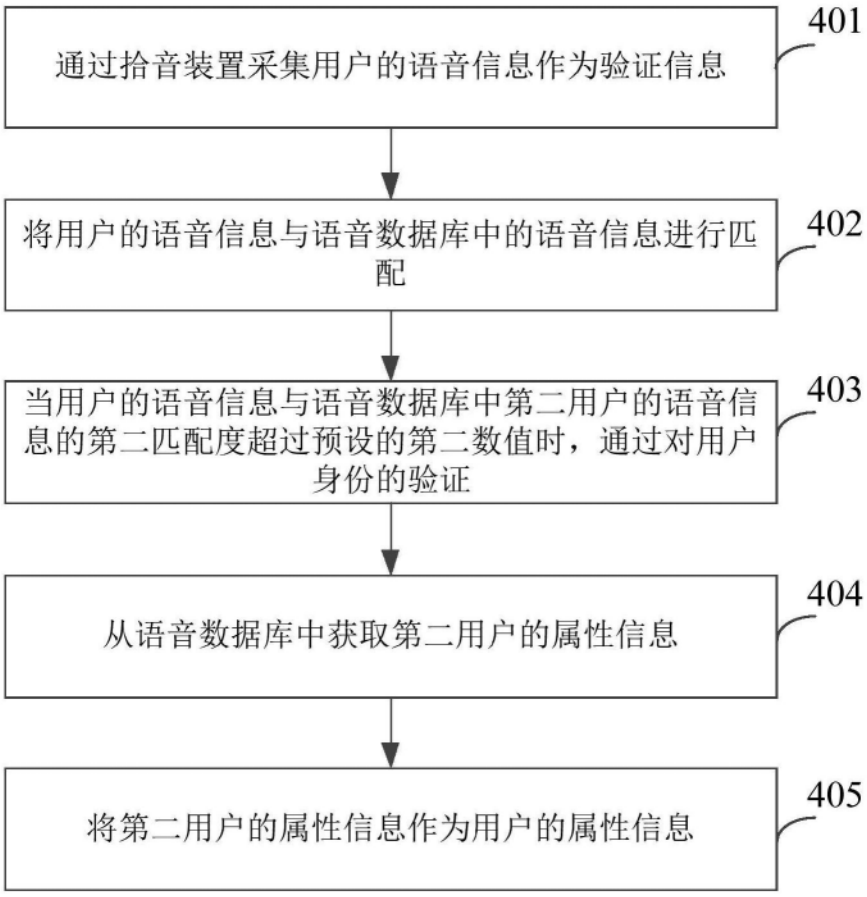

401
通过拾音装置采集用户的语音信息作为验证信息
402
将用户的语音信息与语音数据库中的语音信息进行匹配
403
当用户的语音信息与语音数据库中第二用户的语音信息的第二匹配度超过预设的第二数值时，通过对用户身份的验证
404
从语音数据库中获取第二用户的属性信息
405
将第二用户的属性信息作为用户的属性信息

图7

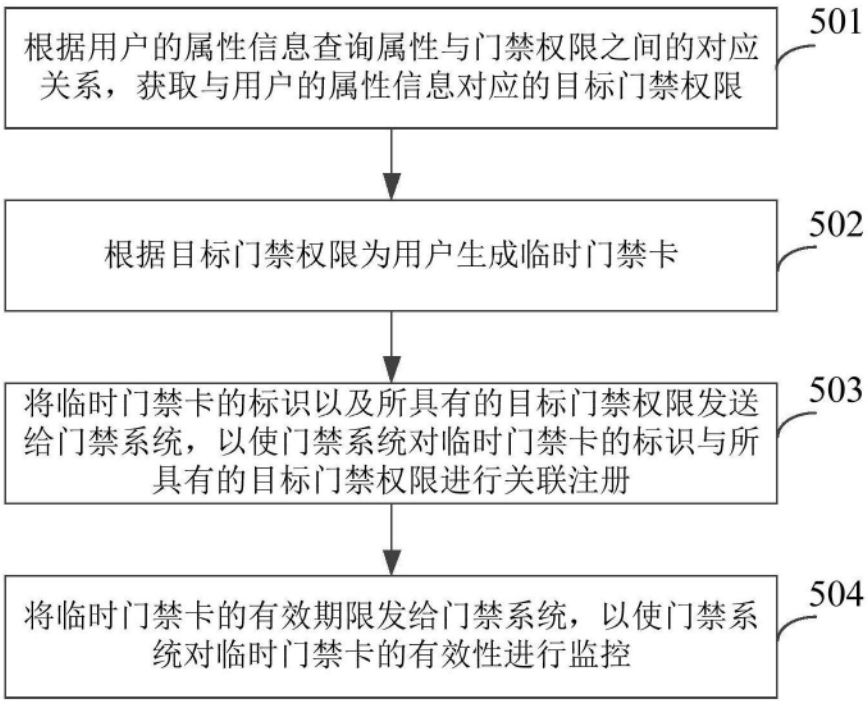

根据用户的属性信息查询属性与门禁权限之间的对应关系，获取与用户的属性信息对应的目标门禁权限
501
根据目标门禁权限为用户生成临时门禁卡
502
将临时门禁卡的标识以及所具有的目标门禁权限发送给门禁系统，以使门禁系统对临时门禁卡的标识与所具有的目标门禁权限进行关联注册
503
将临时门禁卡的有效期限发给门禁系统，以使门禁系统对临时门禁卡的有效性进行监控
504

图8

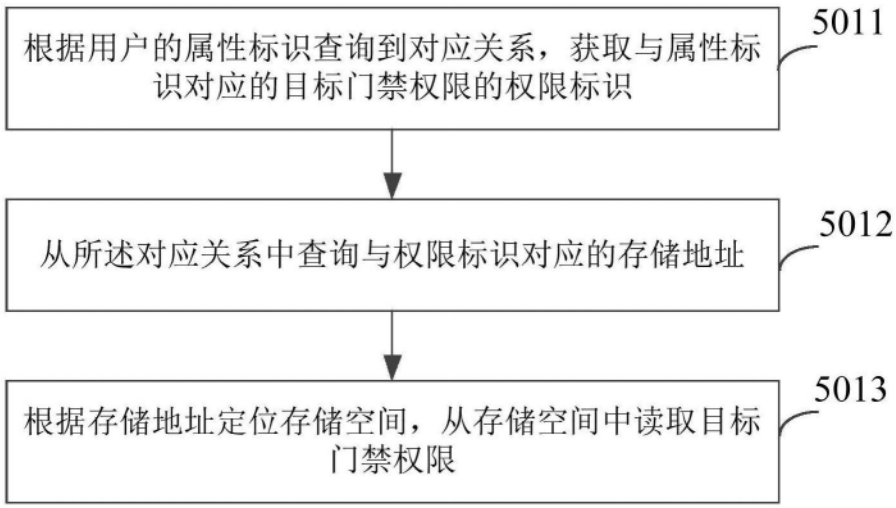

根据用户的属性标识查询到对应关系，获取与属性标识对应的目标门禁权限的权限标识
5011
从所述对应关系中查询与权限标识对应的存储地址
5012
根据存储地址定位存储空间，从存储空间中读取目标门禁权限
5013

图9

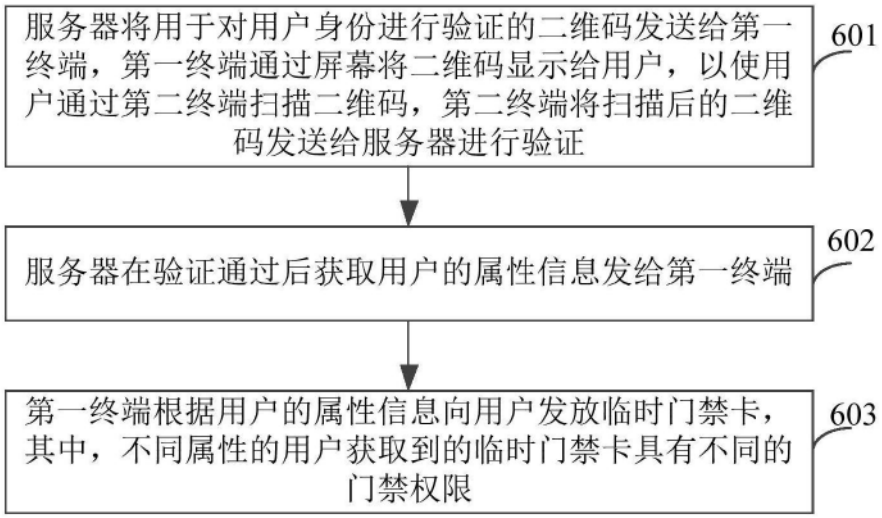

服务器将用于对用户身份进行验证的二维码发送给第一终端，第一终端通过屏幕将二维码显示给用户，以使用户通过第二终端扫描二维码，第二终端将扫描后的二维码发送给服务器进行验证
601
服务器在验证通过后获取用户的属性信息发给第一终端
602
第一终端根据用户的属性信息向用户发放临时门禁卡，其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限
603

图10


欢迎到XX公司
已约访客
员工启动

图11

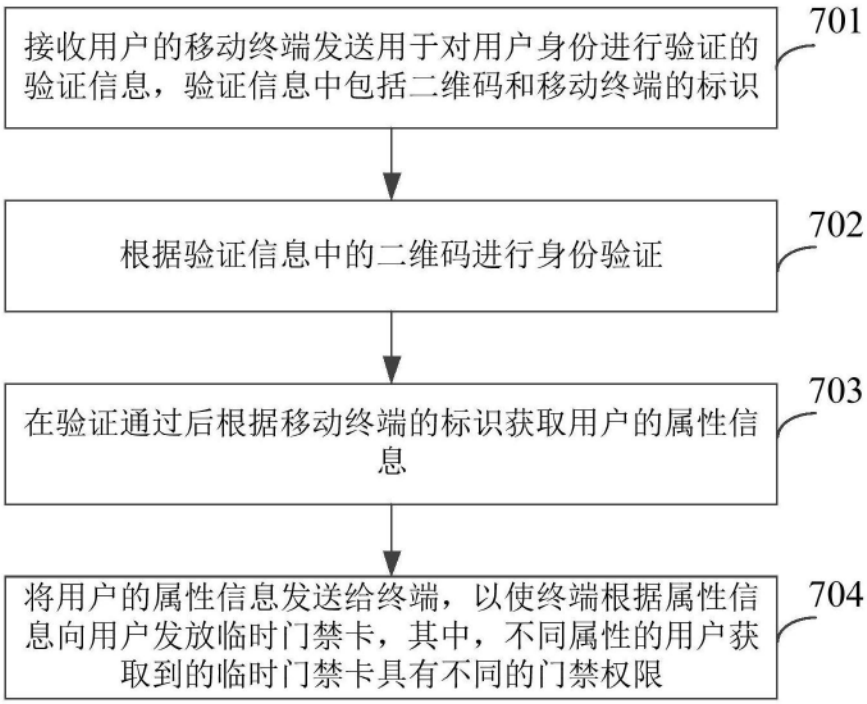

接收用户的移动终端发送用于对用户身份进行验证的验证信息，验证信息中包括二维码和移动终端的标识
701
根据验证信息中的二维码进行身份验证
702
在验证通过后根据移动终端的标识获取用户的属性信息
703
将用户的属性信息发送给终端，以使终端根据属性信息向用户发放临时门禁卡，其中，不同属性的用户获取到的临时门禁卡具有不同的门禁权限
704

图12

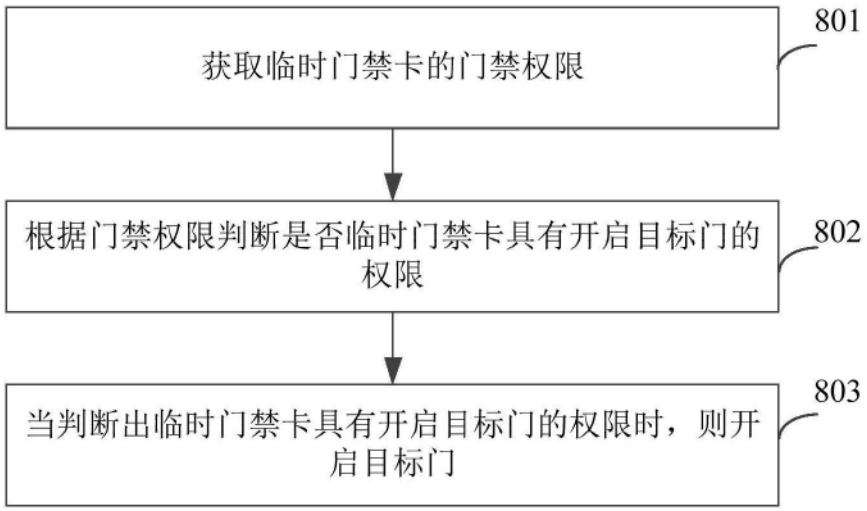

获取临时门禁卡的门禁权限
801
根据门禁权限判断是否临时门禁卡具有开启目标门的权限
802
当判断出临时门禁卡具有开启目标门的权限时，则开启目标门
803

图13

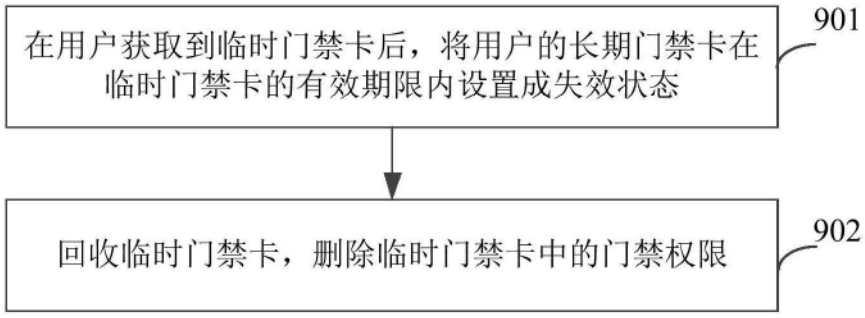

在用户获取到临时门禁卡后，将用户的长期门禁卡在临时门禁卡的有效期限内设置成失效状态
901
回收临时门禁卡，删除临时门禁卡中的门禁权限
902

图14

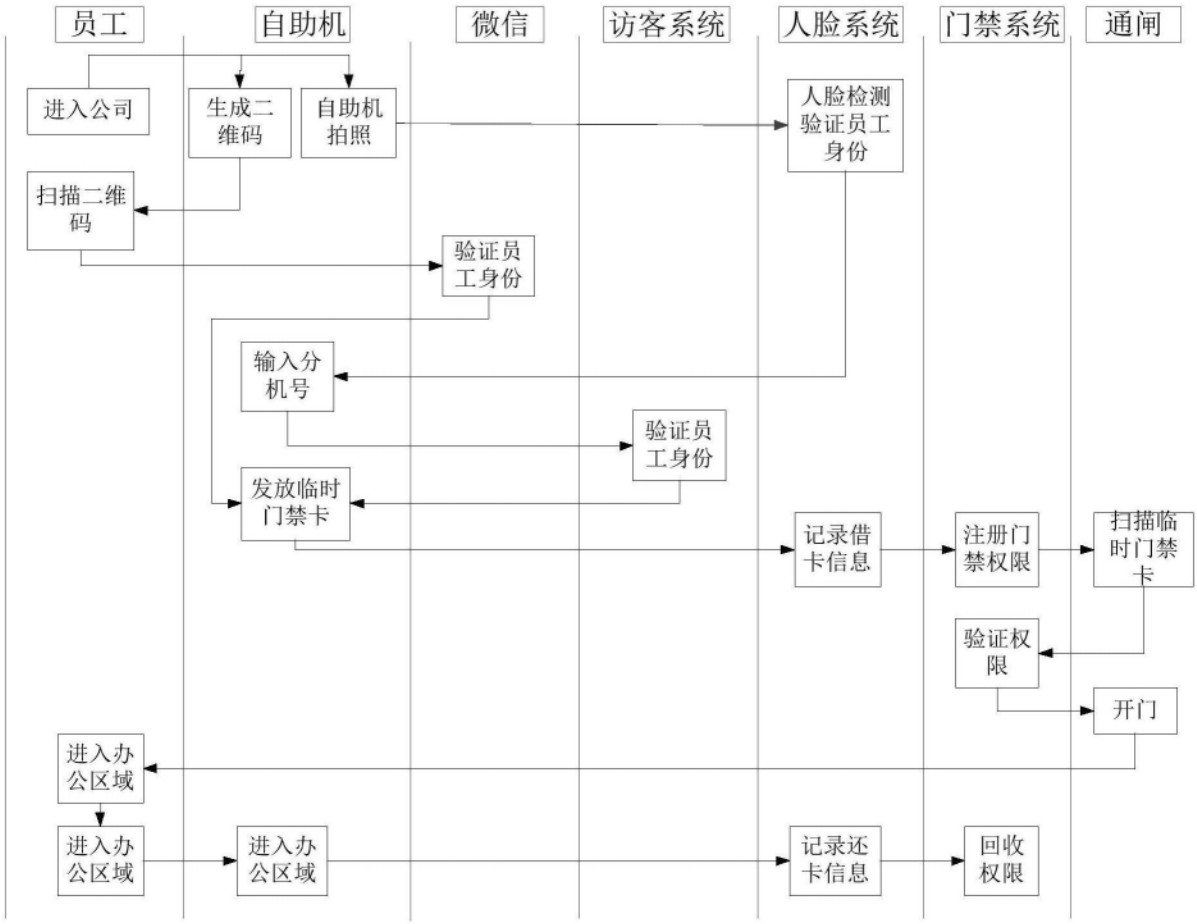

员工
自助机
微信
访客系统
人脸系统
门禁系统
通闸
进入公司
生成二维码
自助机拍照
人脸检测验证员工身份
扫描二维码
验证员工身份
输入分机号
验证员工身份
发放临时门禁卡
记录借卡信息
注册门禁权限
扫描临时门禁卡
验证权限
开门
进入办公区域
进入办公区域
进入办公区域
记录还卡信息
回收权限

图15

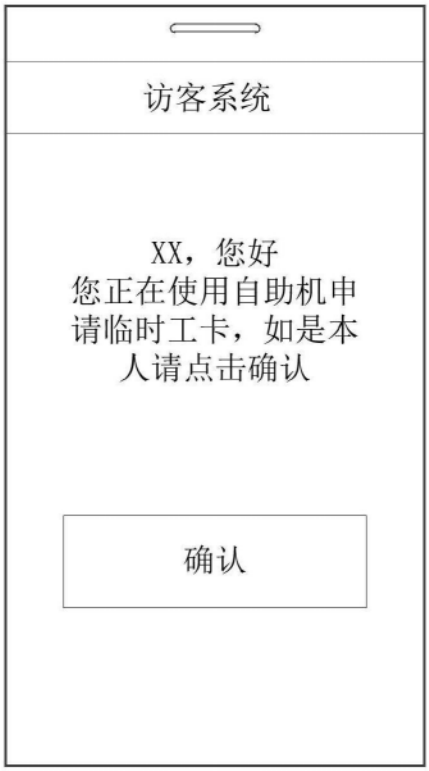

访客系统
XX，您好
您正在使用自助机申请临时工卡，如是本人请点击确认
确认

图16 (a)


请输入五位数的分机号
7
8
9
X
4
5
6
清空
7
7
7
确认
0

图16 (b)

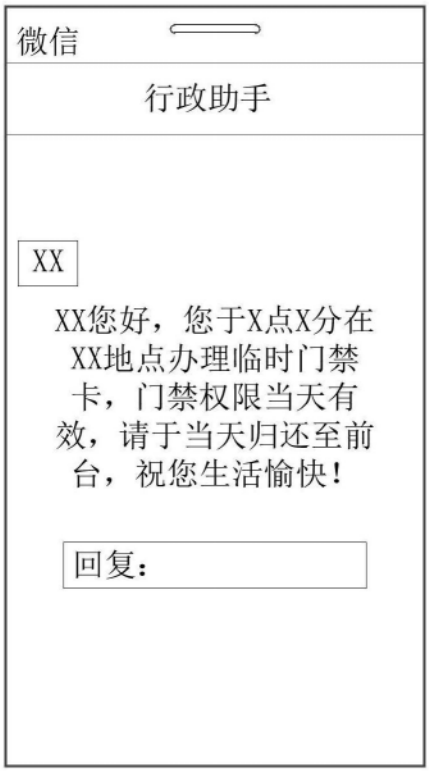

微信
行政助手
XX
XX您好，您于X点X分在XX地点办理临时门禁卡，门禁权限当天有效，请于当天归还至前台，祝您生活愉快！
回复：

图16(c)

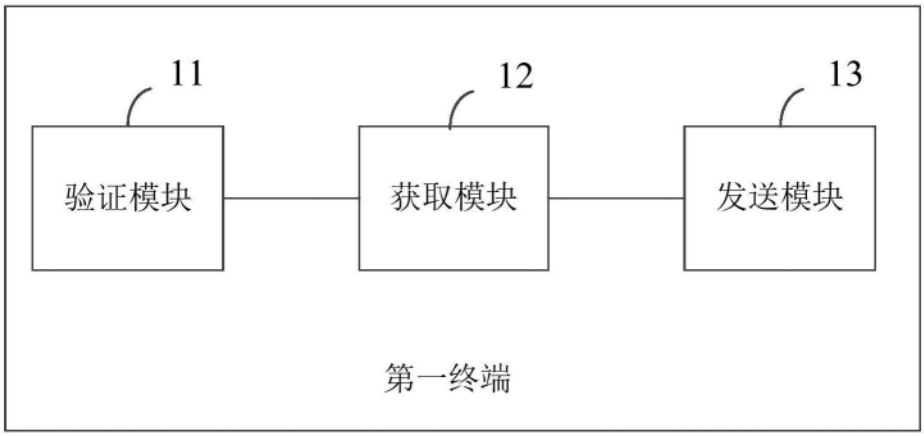

11
12
13
验证模块
获取模块
发送模块
第一终端

图17

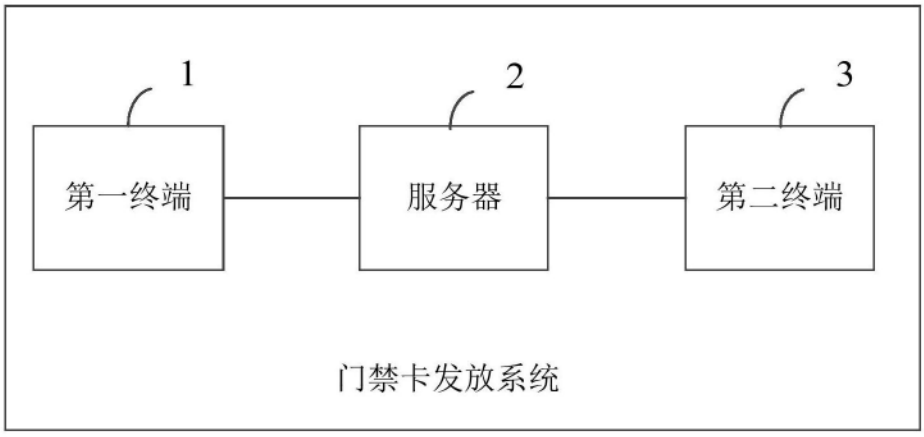


图18

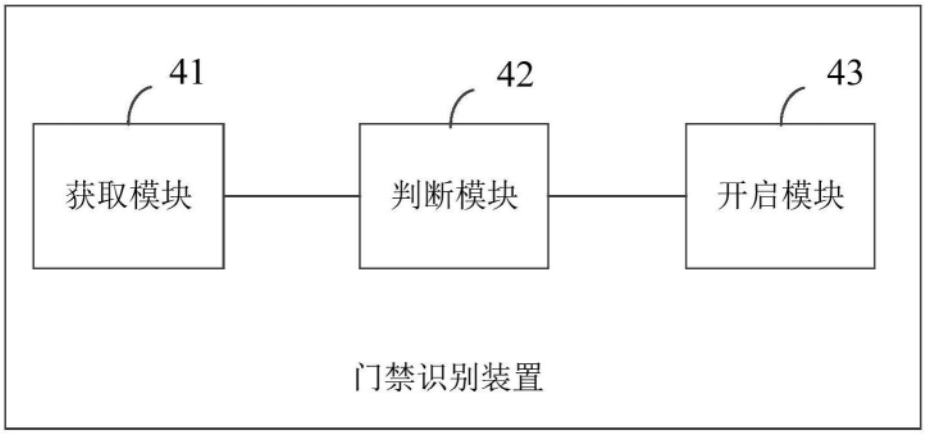


图19

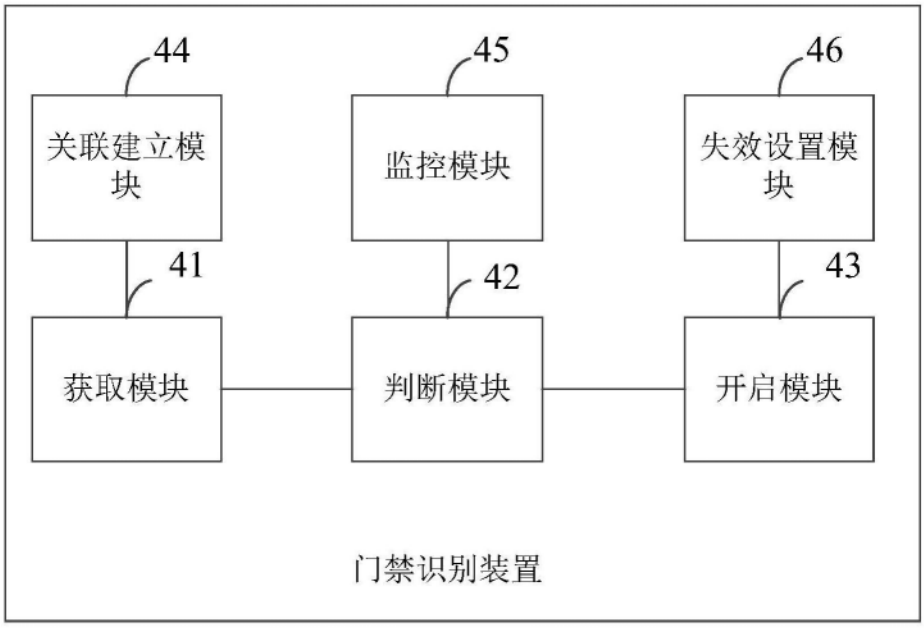

44
45
46
关联建立模块
监控模块
失效设置模块
41
42
43
获取模块
判断模块
开启模块
门禁识别装置

图20

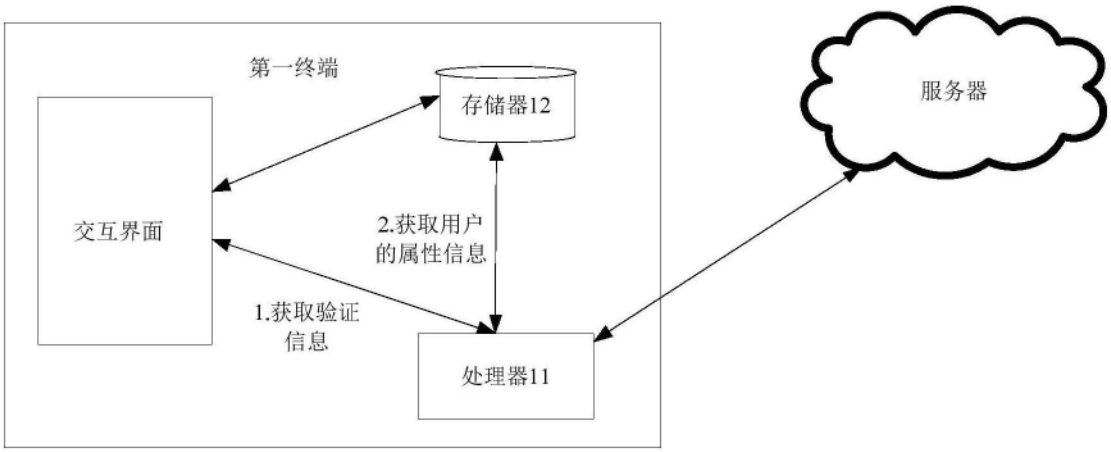

第一终端
存储器12
服务器
交互界面
2.获取用户的属性信息
1.获取验证信息
处理器11

图21

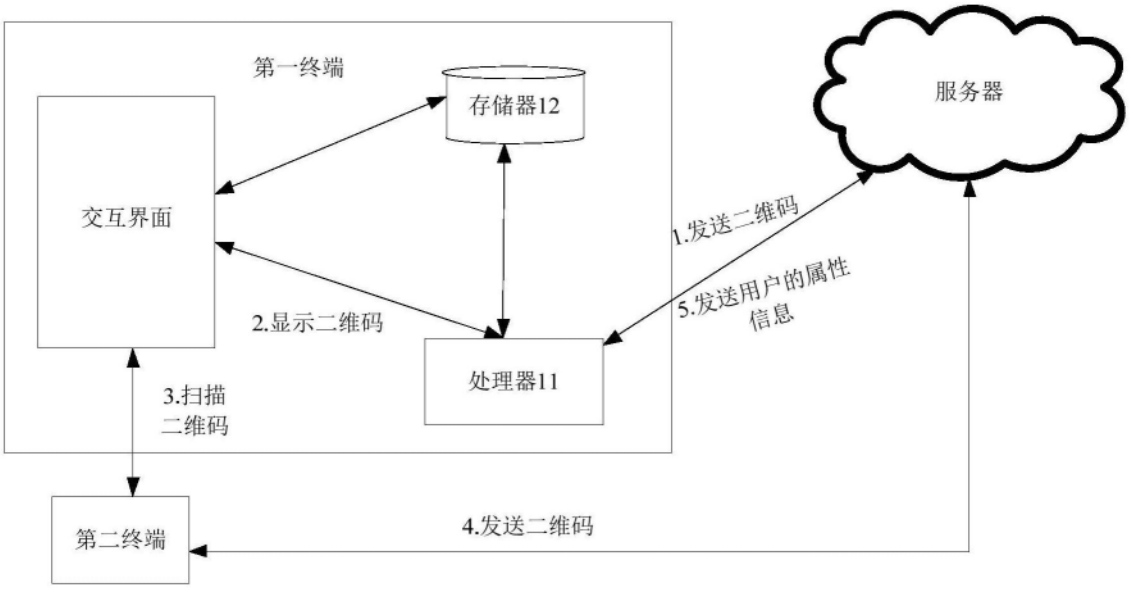

第一终端
存储器12
交互界面
服务器
1.发送二维码
5.发送用户的属性信息
2.显示二维码
处理器11
3.扫描二维码
第二终端
4.发送二维码

图22

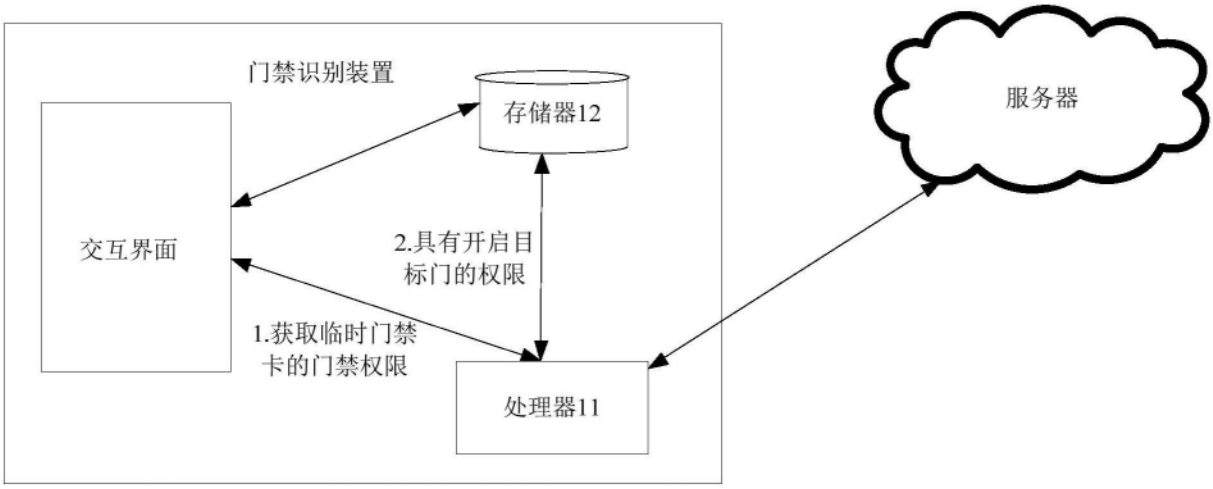

门禁识别装置
存储器12
服务器
交互界面
2.具有开启目标门的权限
1.获取临时门禁卡的门禁权限
处理器11

图23